



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,511	01/04/2002	Andrew Brown	COMP.0268 P01-3942	6225
7590	09/27/2005		EXAMINER	
Intellectual Property Administration Legal Dept., M/S 35 P.O. Box 272400 Ft. Collins, CO 80527-2400			SHIFERAW, ELENI A	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 09/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/037,511	BROWN ET AL.
	Examiner	Art Unit
	Eleni A. Shiferaw	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 30 June 2005.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-20 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 04 January 2002 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____

Detailed Action
Response to Amendment

1. Applicant's arguments with respect to claims 1-20 have been fully considered but are moot in view of the new ground(s) of rejection.
2. Claims 1-20 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saarinen (Pub. No.: US 2002/0172359 A1) in view of Kara (Patent Number: 5,802,175) and Nordqvist et al. (Nordqvist, Pub. No.: US 2002/0191799 A1).

As per claim 1, Saarinen teaches a method of ensuring a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of:

obtaining a seed pool comprising a plurality of bits for generating the random number (Saarinen page 2 par. 0022 lines 7-10 and par. 0014);

Saarinen doesn't explicitly teach remotely storing seed pool;

However **Kara** discloses: remotely storing a seed pool via a network (Kara col. 6 lines 3-15, Kara col. 3 lines 51-58 and col. 2 lines 43-46; portable memory device/Touch Memory remotely providing/storing seed values for key generation to PC/processor-based); and

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to remotely seeding starting values to generate session key because it would securely transmit/store seed values remotely through computer network and/or telecommunications for key generation and decryption of data.

Saarinen and Kara fail to explicitly disclose restoring the seed pool backup to local memory following a power loss event causing loss to the seed pool.

However **Nordqvist** discloses restoring the seed pool backup to local memory following a power loss event causing loss to the seed pool (Nordqvist page 2 par. 0023; retaining/restoring/repopulating data/initial value/algorithm stored on RAM/power dependent memory during power interruptions/loss or removal of battery and loss of data).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nordqvist within the combination system of Saarinen and Kara because it is well known to backup a data during battery replacement or power/data loss. One would have been motivated to incorporate the teachings of bucking up data/seed because it would retain/replace the seed data during battery replacement or power interruptions (Nordqvist page 2 par. 0023).

As per claim 11, Saarinen teaches a method of restoring a seed pool for generating a random number for a security system, the method comprising the acts of:

transmitting a periodically the seed pool to the security system (Saarinen page 4 par. 0071; periodically re-seeding upon each new instance of new input entropy);

seed pool for use in generating the random number (Saarinen page 2 par. 0022 lines 7-10 and fig. 5B element 518);

Saarinen doesn't explicitly teach remotely seeding or storing of seed values remotely;

However **Kara** discloses: transmitting seed pool to the security system via a network (Kara col. 6 lines 3-15, Kara col. 3 lines 51-58 and col. 2 lines 43-46; portable memory device/Touch Memory remotely providing seed values for key generation); and

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to remotely seeding starting values to generate session key because it would securely transmit seed values remotely through computer network and/or telecommunications for key generation and decryption of data.

Saarinen and Kara fail to explicitly disclose repopulating local memory of the security system with the stored backup following loss of the seed pool;

However Nordqvist discloses:

transmitting a periodically stored backup of the seed pool (*initial value or algorithm or data*) to the security system following loss of the seed pool from the security system (Nordqvist page 2 par. 0023; retaining/restoring/repopulating data/initial value/algorithm stored on RAM/power dependent memory during power interruptions/loss or removal of battery and loss of data); and

repopulating local memory of the security system with the stored backup (Nordqvist page 2 par. 0023; retaining/restoring/repopulating data/initial value/algorithm stored on RAM/power dependent memory during power interruptions/loss or removal of battery and loss of data).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nordqvist within the combination system of Saarinen and Kara because it is well known to backup a data during battery replacement or power/data loss. One would have been motivated to incorporate the teachings of bucking up data/seed because it would retain/replace the seed data during battery replacement or power interruptions (Nordqvist page 2 par. 0023).

As per claim 17, Saarinen teaches a security system, comprising:

a security subsystem, comprising:

a power dependent memory device (Saarinen page 3 par. 0030);

a limited life battery for the power dependent memory device (Saarinen page 3 par. 0030);

a seed pool stored on the power dependent memory device, wherein the seed pool comprises a plurality of random bits (Saarinen page 2 par. 0014); and

security logic configured to generate a cryptographic key to establish a secure communication session between the electronic device and an external device, wherein the security logic generates the cryptographic key from the seed pool (Saarinen page 1 par. 0002 and page 2 par. 0022 lines 7-10; generation of session key from seed); and

a control module configured for periodically storing the seed pool in the remote storage device (Saarinen page 4 par. 0071; periodically re-seeding upon each new instance of new input entropy);

Saarinen doesn't explicitly teach remotely seeding or storing of seed values remotely;

However **Kara** discloses: a security system, comprising:

a remote storage device (Kara col. 6 lines 3-15, Kara col. 3 lines 51-58 and col. 2 lines 43-46; portable memory device/Touch Memory remotely providing seed values for key generation); and

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to remotely seeding starting values to generate session key because it would securely transmit seed values remotely through computer network and/or telecommunications for key generation and decryption of data.

Saarinen and Kara fail to explicitly disclose backup following replacement of the limited life battery.

However **Nordqvist** discloses a restoration control module configured for repopulating the power dependent memory device with the backup following replacement of the limited life battery (Nordqvist page 2 par. 0023; retaining/restoring/repopulating data/initial value/algorithm stored on RAM/power dependent memory during power interruptions/loss or removal of battery and loss of data).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nordqvist within the combination system of Saarinen and Kara because it is well known to backup a data during battery replacement or power loss. One would have been motivated to incorporate the teachings of bucking up data/seed because it would retain/replace the seed data during battery replacement or power interruptions (Nordqvist page 2 par. 0023).

As per claim 2, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition the combination teach the method, wherein the act of remotely storing the seed pool comprises the act of periodically storing the seed pool backup on a remote storage device (Saarinen page 4 par. 0071; periodically re-seeding upon each new instance of new input entropy and Kara col. 6 lines 3-15, and col. 2 lines 43-46). The rational for combining are the same as claim 1 above.

As per claims 3 and 14, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition the combination teaches the method wherein the act of periodically storing the seed pool backup comprising the act of periodically storing the seed pool in a remote storage device via the network at an interval based on a write cycle characteristic of the remote storage device to maintain availability of the seed pool as the periodically stored backup (Saarinen page 3 par. 0033 lines 7-10 and Kara col. 6 lines 3-15, and col. 2 lines 43-46). The rational for combining are the same as claim 1 above.

As per claim 4, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition Saarinen teaches the method, comprising the act of modifying the seed pool backup with additional random bits to ensure randomness for generating the random number (Saarinen page 1 par. 0003 lines 5-7 and par. 0007-0008).

As per claim 5, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In

addition Saarinen teaches the method, wherein the act of modifying the seed pool backup with additional random bits comprises the act of capturing one or more bits of data from a free-running timer (Saarinen page 1 par. 0003 lines 5-7 and par. 0007-0008).

As per claims 6 and 13, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition Saarinen teaches the method, wherein the act of modifying the seed pool backup with additional random bits comprises the act of capturing one or more bits of data from a local hardware device (Saarinen page 2 par. 0014).

As per claim 7, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition the combination teaches the method, wherein the act of restoring the seed pool backup comprises the act of automatically retrieving the seed pool backup via the network upon restoring power to the cryptographic security subsystem (Nordqvist page 2 par. 0023, and Kara col. 6 lines 3-15, and col. 2 lines 43-46). The rational for combining are the same as claim 1 above.

As per claim 8, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition the combination teach the method, wherein the act of automatically retrieving the seed pool backup comprises requesting the seed pool backup from a remote management system (Kara col. 6 lines 3-15, and col. 2 lines 43-46 and Nordqvist page 2 par. 0023). The rational for combining are the same as claim 1 above.

As per claim 9, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition Nordqvist teaches the method, wherein the power loss event is a battery failure resulting in memory loss of the seed pool from the local memory (Nordqvist page 2 par. 0023). The rational for combining are the same as claim 1 above.

As per claim 10, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition the combination teach the method, wherein the act of restoring the seed pool backup comprises the act of transmitting the seed pool backup from remote storage to the local memory via the network following a battery replacement for the local memory (Nordqvist page 2 par. 0023, and Kara col. 3 lines 51-58). The rational for combining are the same as claim 1 above.

As per claim 12, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, Saarinen teaches the method, comprising the act of modifying the periodically stored backup with additional random bits to ensure randomness (Saarinen page 1 par. 0003 lines 5-7 and par. 0007-0008).

As per claim 15, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, Nordqvist teaches the method, wherein the act of transmitting the periodically stored backup comprises the act of transferring the periodically stored backup to the security system after restoring battery power to the security system (Nordqvist page 2 par. 0023). The rational for combining are the same as claim 11 above.

As per claim 16, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, the combination teach the method, wherein the act of transferring the periodically stored backup comprises automatically initiating a seed pool restoration event using the periodically stored backup stored on a remote server after restoring battery power by replacing a battery for the local memory of the security system (Nordqvist page 2 par. 0023, and Kara col. 3 lines 51-57). The rational for combining are the same as claim 11 above.

As per claim 18, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, Kara teaches the system, comprising a remote security interface configured for interacting with the security subsystem and the security backup system (Kara col. 2 lines 46-52, and col. 3 lines 51-57). The rational for combining are the same as claim 17 above.

As per claim 19, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, the combination teach the system, wherein the security backup system comprises a seed pool modification module configured for capturing one or more bits of data from a hardware component and adding the one or more bits to the backup (Saarinen page 3 col. 0035-0038 and Nordqvist page 2 par. 0023). The rational for combining are the same as claim 18 above.

As per claim 20, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, Nordqvist teaches the system, wherein the security backup system comprises an automation module configured for automatically initiating repopulation of the memory device

with the backup (Nordqvist page 2 par. 0023). The rational for combining are the same as claim 18 above.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Eleni Shiferaw
September 22, 2005

ell
Primary Examiner
Art Unit
9123bs